Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Account Credentials Management Policy:

PURPOSE:
This policy establishes standards for administering user account credentials that access Clarendon College's information technology resources. These resources must be protected from unauthorized access, loss, corruption, or destruction, thus ensuring these resources' confidentiality, integrity, and availability. Proper management of account credentials provides a means of assuring accountability and protecting Clarendon College's resources. The standards established in this policy include issuing account credentials, granting access to approved resources, account credential maintenance, and deactivation processes.

Scope:
The Clarendon College User Account Credentials Management policy applies to those responsible for managing user account credentials on Clarendon College's information technology resources.

Policy Statement:
Creating unique domain user account credentials is an automated process utilizing the current approved Clarendon College account naming convention and is based on assigned roles within the Enterprise Resource Planning (ERP) system (e.g., faculty, staff, student worker, student, visitor, alums, etc.) The level of authorized access will be based on the principle of least privilege (PoLP), but if a user is assigned multiple roles, the most privileged role will take precedence.

1. Creating a user account credential issues, a unique, non-transferable electronic identity known as the “username” and a corresponding “password.” Usernames will remain in effect throughout the individual’s official affiliation with Clarendon College. (User Account Password Policy).
2. Usernames are not reused.
3. When an individual changes role or ends their affiliation, Clarendon College-IT deactivates the user account credentials that no longer meet Clarendon College's eligibility requirements (User Account Management Policy) and removes non-standard access.
4. Upon user activation, account holders can access the resources their role membership dictates.
5. Clarendon College-IT requires users to change passwords per the User Account Password Policy.
6. Requests for exceptions to this policy must be submitted in writing (Clarendon College-Compliance Policy and Exception Form) to the Information Security Officer (ISO) or Vice President of Information Technology. They will be reviewed on a case-

by-case basis. Requests shall be justified, documented, and communicated during the risk assessment.

Definition:

Enterprise Resource Planning (ERP): is a software system that helps businesses manage their core processes, such as accounting, procurement, and supply chain. ERP systems can improve efficiency and decision-making.

Principle of Least Privilege (PoLP): is an information security concept that maintains that a user or entity should only have access to the specific data, resources, and applications needed to complete a required task.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.